THE ACM DIGITAL LIBRARY — Advanced Search

Search Tips

Enter words, phrases or names below. Surround phrases or full names with double quotation marks.

Desired Results:

must have **all** of the words or phrases

Cash "private key" "public key"

must have **any** of the words or phrases

"digital cash" " virtual cash" " digicash" "electronic ca

must have **none** of the words or phrases

Name or Affiliation:

Authored by: all any none

Edited by: all any none

Reviewed by: all any none

Only search in:*

Title Abstract Review All Information

SEARCH

*Searches will be performed on all available information, including full text where available, unless specified above.

ISBN / ISSN: Exact Expand

DOI: Exact Expand

SEARCH

Published:

By: all any none

In: all any none

Since: Month Year

Before: January 2001

As: Any type of publication

Conference Proceeding:

Sponsored By:

Conference Location:

Conference Year: yyyy

SEARCH

Classification: (CCS) Primary Only

Classified as: all any none

Subject Descriptor: all any none

Keyword Assigned: all any none

Results must have accessible:

Full Text Abstract Review

h c g e ch cf c

SEARCH

h c g e ch cf c

Published before January 2001
Terms used **Cash private key public key digital cash virtual cash digicash electronic cash**

Found **20** of **109,225**

Sort results by: relevance
Display results: expanded form

Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 20

Relevance scale

1 Money in electronic commerce: digital cash, electronic fund transfer, and Ecash
Patiwat Panurach
June 1996 **Communications of the ACM**, Volume 39 Issue 6
Full text available: pdf(551.73 KB) Additional Information: full citation, references, citings, index terms, review

2 Atomicity in electronic commerce
J. D. Tygar
May 1996 **Proceedings of the fifteenth annual ACM symposium on Principles of distributed computing**
Full text available: pdf(1.74 MB) Additional Information: full citation, references, citings, index terms

3 Revokable and versatile electronic money (extended abstract)
Markus Jakobsson, Moti Yung
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**
Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

4 Ticket based service access for the mobile user
Bhrat Patel, Jon Crowcroft
September 1997 **Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking**
Full text available: pdf(1.52 MB) Additional Information: full citation, references, citings, index terms

5 Unlinkable serial transactions: protocols and applications
Stuart G. Stubblebine, Paul F. Syverson, David M. Goldschlag
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4
Additional Information: full citation, abstract, references, citings, index

Full text available: pdf(184.87 KB) terms, review

We present a protocol for unlinkable serial transactions suitable for a variety of network-based subscription services. It is the first protocol to use cryptographic blinding to enable subscription services. The protocol prevents the service from tracking the behavior of its customers, while protecting the service vendor from abuse due to simultaneous or cloned use by a single subscriber. Our basic protocol structure and recovery protocol are robust against failure in protocol termination. ...

Keywords: anoymity, blinding, cryptographic protocols, unlinkable serial transactions

6 Untraceability in mobile networks

Didier Samfat, Refik Molva, N. Asokan

December 1995 **Proceedings of the 1st annual international conference on Mobile computing and networking**

Full text available: pdf(1.20 MB) Additional Information: full citation, references, citings, index terms

Keywords: CDPD, GSM, alias, anonymity, authentication, location privacy, mobility, security

7 Anonymous credit cards

Steven H. Low, Sanjoy Paul, Nicholas F. Maxemchuk

November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security**

Full text available: pdf(871.53 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes a communications networking technique for funds transfer which combines the privacy of cash transactions with the security, record-keeping and charging mechanisms of credit cards. The scheme uses a communications network and cryptographic protocols to separate information. The company that extends credit to the individual and collects the bill does not have access to the specific purchases, and the shop that sells the merchandise is convinced that it will be paid withou ...

8 Market-based resource control for mobile agents

Jonathan Bredin, David Kotz, Daniela Rus

May 1998 **Proceedings of the second international conference on Autonomous agents**

Full text available: pdf(1.11 MB) Additional Information: full citation, references, citings, index terms

9 Untraceable off-line electronic cash flow in e-commerce

H. Wang, Y. Zhang

January 2001 **Australian Computer Science Communications , Proceedings of the 24th Australasian conference on Computer science**, Volume 23 Issue 1

Full text available: pdf(791.70 KB) Publisher Site Additional Information: full citation, abstract, references, citings

Electronic cash has been playing an important role in electronic - commerce. One of the desirable characteristics is its traceability, which can prevent money laundering and can find the destination of suspicious withdrawals.In this paper we develop a new scheme for untraceable electronic cash, in which the bank involvement in the payment transaction between a user and a receiver is eliminated. The user withdraws electronic "coins" from the

bank and uses them to pay to a receiver. The receiver s ...

Keywords: DLA, cut-and-choose technique, electronic-cash, hash function, random oracle model

10 A new on-line cash check scheme
Robert H. Deng, Yongfei Han, Albert B. Jeng, Teow-Hin Ngair
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security**
Full text available: pdf(690.98 KB) Additional Information: full citation, references, index terms

11 Trustee-based tracing extensions to anonymous cash and the making of anonymous change
Ernie Brickell, Peter Gemmell, David Kravitz
January 1995 **Proceedings of the sixth annual ACM-SIAM symposium on Discrete algorithms**
Full text available: pdf(1.11 MB) Additional Information: full citation, references, citings, index terms

12 Conditional purchase orders
John Kelsey, Bruce Schneier
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security**
Full text available: pdf(853.77 KB) Additional Information: full citation, references, index terms

13 NetCash: a design for practical electronic currency on the Internet
Gennady Medvinsky, Clifford Neuman
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**
Full text available: pdf(604.22 KB) Additional Information: full citation, abstract, references, citings, index terms

Licensing is a topic of increasing importance for software publishers and users. More and more, the magnitude of financial transfers between these two partners are determined by some electronic licensing service being part of the system on which the licensed software is running. In order to ease the use and management of such licensing schemes and to enable economic software usage in enterprise-wide computer systems through flexible and fair billing structures, various organizations are wor ...

14 A long-term perspective on electronic commerce
Eric Hughes
November 1997 **netWorker**, Volume 1 Issue 3
Full text available: pdf(535.69 KB) Additional Information: full citation, references, index terms

15 Distributed digital-ticket management for rights trading system
Kazuo Matsuyama, Ko Fujimura
November 1999 **Proceedings of the 1st ACM conference on Electronic commerce**
Full text available: Additional Information:

h c g e cf

pdf(152.63 KB) full citation, references, index terms

Keywords: account, circulation, coupon, digital ticket, protocol, rights, smart card, trading system

16 A secure marketplace for mobile Java agents
Kay Neuenhofen, Matthew Thompson
May 1998 **Proceedings of the second international conference on Autonomous agents**
Full text available: pdf(889.69 KB) Additional Information: full citation, references, citings, index terms

Keywords: agent architectures, mobile agents, security

17 Fair exchange with a semi-trusted third party (extended abstract)
Matthew K. Franklin, Michael K. Reiter
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security**
Full text available: pdf(869.47 KB) Additional Information: full citation, references, citings, index terms

18 A new family of authentication protocols
Ross Anderson, Francesco Bergadano, Bruno Crispo, Jong-Hyeon Lee, Charalampos Manifavas, Roger Needham
October 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 4
Full text available: pdf(821.42 KB) Additional Information: full citation, abstract, index terms

We present a related family of authentication and digital signature protocols based on symmetric cryptographic primitives which perform substantially better than previous constructions. Previously, one-time digital signatures based on hash functions involved hundreds of hash function computations for each signature; we show that given online access to a timestamping service, we can sign messages using only two computations of a hash function. Previously, techniques to sign infinite streams invol ...

Keywords: authentication, hashing, non-repudiation, timestamping

19 Funkspiel schemes: an alternative to conventional tamper resistance
Johan Håstad, Jakob Jonsson, Ari Juels, Moti Yung
November 2000 **Proceedings of the 7th ACM conference on Computer and communications security**
Full text available: pdf(528.32 KB) Additional Information: full citation, references, citings, index terms

20 On secure and pseudonymous client-relationships with multiple servers
Eran Gabber, Phillip B. Gibbons, David M. Kristol, Yossi Matias, Alain Mayer
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4
Full text available: pdf(161.56 KB) Additional Information: full citation, abstract, references, citings, index terms, review

This paper introduces a cryptographic engine, Janus, which assists clients in establishing and maintaining secure and pseudonymous relationships with multiple servers. The setting is such that clients reside on a particular subnet (e.g., corporate intranet, ISP) and the servers reside anywhere on the Internet. The Janus engine allows each client-server relationship to use either weak or strong authentication on each interaction. At the same time, each interaction preserves privacy by neithe ...

Keywords: Janus function, anonymity, mailbox, persistent relationship, privacy, pseudonym

Results 1 - 20 of 20

h c g e cf